## CLAIMS

What is claimed is:

1. A method comprising:

requesting a service for a platform;

certifying the use of the service for one or more acceptable configurations of the platform; and

receiving a session key for a session of the service, the service being limited to the one or more acceptable configurations of the platform.

2. The method of claim 1, further comprising obtaining an identifying credential.

3. The method of claim 2, wherein the identifying credential comprises an attestation identification key (AIK) certificate.

4. The method of claim 2, wherein the identifying credential is obtained from a trusted third party.

5. The method of claim 2, wherein the identifying credential is obtained through a transaction with the service provider.

6. The method of claim 1, wherein certifying the use of the service comprises producing hash data relating to the one or more acceptable configurations.

7. The method of claim 1, wherein certifying the use of the service comprises confirming that a chosen configuration is included in a set of values representing the one or acceptable configurations.

8. A method comprising:

receiving a service request from a client for a platform;

creating a service key generation request for the client;

validating the service key, validation of the service key comprising receipt of assurance that the service is used only for one or more acceptable configurations for the platform; and

providing a session key to the client based on the validated service key, the session key being limited to the one or more acceptable configurations.

9. The method of claim 8, further comprising receiving an identifying credential from the client.

10. The method of claim 9, wherein the identifying credential comprises an attestation identification key (AIK) certificate.

11. The method of claim 8, wherein validating the service key comprises sending a certification request to the client and receiving hash data relating to the one or more acceptable configurations.

12. The method of claim 8, wherein validating the service key comprises sending a list of value sets for the one or more acceptable configurations to the client and receiving a confirmation that a chosen configuration is included in the list of value sets.

13. A client device comprising:

a communication device to communicate with a service provider, the client device to request a service from the service provider for a platform; and

a trusted platform module (TPM) to provide secure operations in connection with the service from the service provider;

the client device to provide assurance to the service provider that the service is limited to one or more acceptable configurations for the platform.

14. The client device of claim 13, wherein the provision of assurance to the service provider comprises receiving a certification request from the service provider, producing hash data relating to the one or more acceptable configurations using the trusted platform module, and sending the hash data to the service provider.

15. The client device of claim 13, wherein the provision of assurance to the service provider comprises receiving a list of acceptable value sets relating to the one or more acceptable configurations and sending a confirmation that a chosen configuration is included in the list of acceptable value sets.

16. A system comprising;

a client device, the client device comprising a trusted platform module; and

a service provider to provide a service to the client device;

the client device to certify that the service will be utilized only in one or more acceptable configurations of a platform of the client device.

17. The system of claim 16, wherein the client device obtains an identifying credential.

18. The system of claim 17, wherein the identifying credential comprises an attestation identification key (AIK) certificate.

19. The system of claim 17, wherein the identifying credential is obtained from a trusted third party.

20. The system of claim 17, wherein the identifying credential is obtained through a transaction with the service provider.

21. The system of claim 16, wherein certifying the use of the service comprises producing hash data relating to the one or more acceptable configurations.

22. The system of claim 16, wherein certifying the use of the service comprises confirming that a chosen configuration is included in a set of values representing the one or more acceptable configurations.

23. A machine-readable medium having stored thereon data representing sequences of instructions that, when executed by a processor, cause the processor to perform operations comprising:

requesting a service for a platform;

certifying the use of the service for one or more acceptable configurations of the platform; and

receiving a session key for a session of the service, the service being limited to the one or more acceptable configurations of the platform.

24. The medium of claim 23, wherein certifying the use of the service comprises producing hash data relating to the one or more acceptable configurations.

25. The medium of claim 23, wherein certifying the use of the service comprises confirming that a chosen configuration is included in a set of values representing the one or acceptable configurations.

26. A machine-readable medium having stored thereon data representing sequences of instructions that, when executed by a processor, cause the processor to perform operations comprising:

receiving a service request from a client;

creating a service key generation request for the client;

validating the service key, validation of the service key comprising receipt of assurance that the service is used only for one or more acceptable configurations; and

providing a session key to client based on the validated key, the session key being limited to the one or more acceptable configurations.

27. The medium of claim 26, wherein validating the service key comprises sending a certification request to the client and receiving hash data relating to the one or more acceptable configurations.

28. The medium of claim 27, wherein validating the service key comprises sending a list of value sets for the one or more acceptable configurations to the client and receiving a confirmation that a chosen configuration is included in the list of value sets.